**IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES**

In re Application of:	) **Mail Stop Appeal Brief - Patents**
	)
Shawn E. WIEDERIN et al.	) Group Art Unit: 2132
	)
Application No.: 10/608,137	) Examiner: B. Lanier
	)
Filed: June 30, 2003	)
	)
For: INTEGRATED SECURITY SYSTEM	)

APPEAL BRIEF

U.S. Patent and Trademark Office
Customer Window, Mail Stop Appeal Brief - Patents
Randolph Building
401 Dulany Street
Alexandria, Virginia 22314

Sir:

     This Appeal Brief is submitted in response to the Office Action mailed August 26,

2008 and in support of the Notice of Appeal filed November 26, 2008.

TABLE OF CONTENTS

I.   REAL PARTY IN INTEREST

The real party in interest of the present application, solely for purposes of identifying and avoiding potential conflicts of interest by Board members due to working in matters in which the member has a financial interest, is Verizon Communications Inc. and its subsidiary companies, which currently include Verizon Business Global, LLC (formerly MCI, LLC) and Cellco Partnership (doing business as Verizon Wireless, and which includes as a minority partner affiliates of Vodafone Group Plc). Verizon Communications Inc. or one of its subsidiary companies is an assignee of record of the present application.

II.   RELATED APPEALS AND INTERFERENCES

Appellants are unaware of any related appeals, interferences or judicial proceedings.

III.   STATUS OF CLAIMS

Claims 1, 4-10, 12-16, and 19-22 are pending in this application. Claims 1, 4-10, 12-16, and 19-22 were rejected in the Office Action dated August 26, 2008, and are the subject of the present appeal. Claims 2, 3, 11, and 23-28 were previously canceled without prejudice or disclaimer. Claims 1, 4-10, 12-16, and 19-22 are reproduced in the Claim Appendix of this Appeal Brief.

IV.   STATUS OF AMENDMENTS

No Amendment has been filed subsequent to the Office Action mailed August 26, 2008.

V.   SUMMARY OF CLAIMED SUBJECT MATTER

The following summary of the presently claimed subject matter indicates certain portions of the specification (including the drawings) that provide examples of embodiments of elements of the claimed subject matter. It is to be understood that other portions of the specification not cited herein may also provide examples of embodiments of elements of the claimed subject matter. It is also to be understood that the indicated examples are merely examples, and the scope of the claimed subject matter includes alternative embodiments and equivalents thereof. References herein to the specification are thus intended to be exemplary and not limiting.

Each of the independent claims involved in this appeal is recited below, followed in parenthesis by examples of where support can be found in the specification and drawings for the claimed subject matter. In addition, each dependent claim argued separately below is also summarized in a similar manner.

Claim 1 recites: A device, comprising: at least one interface configured to receive data transmitted via a network (e.g., 120, Fig. 1; pg. 5, lines 2-14); a firewall (e.g., 240, Fig. 2) configured to: receive data from the at least one interface (e.g., 410, Fig. 4; page 14, lines 7-17), determine whether the data potentially contains malicious content (e.g., 420, Fig. 4; page 14, line 18 – page 15, line 4), and identify first data in the received data that potentially contains malicious content (e.g., 420, 440, Fig. 4; page 14, line 18 – page 16, line 2); intrusion detection logic (e.g., 260, Fig. 2) configured to: receive the first data (e.g., 440, Fig. 4; page 15, line 18 – page 16, line 2), and generate report information based on the first data (e.g., 440, Fig. 4; page 15, line 18 – page 16, line 2); and forwarding logic (e.g., 270, Fig. 2) configured to: receive the report information (e.g.,

460, Fig. 4; page 16, lines 3-9), forward the first data for processing by a user application when the report information indicates that the first data does not contain malicious content (e.g., 470, Fig. 4; page 16, lines 3-9), and forward the report information to a remote central management system when the report information indicates that the first data potentially contains malicious content, the report information allowing the remote central management system to make a forwarding decision on behalf of the device (e.g., 510, 520, Fig. 5; page 16, line 20 – page 17, line 11).

Claim 6 recites: The device of claim 5, wherein the anti-virus logic is further configured to identify unsolicited messages (e.g., page 7, line 17 – page 8, line 7).

Claim 7 recites: The device of claim 1, further comprising: a processing device executing the user application, the user application being associated with at least one of video-on-demand, video-based training, on-line gaming, on-line shopping, downloading music files or downloading games (e.g., page 13, lines 15-19).

Claim 10 recites: In a network device configured to receive data transmitted over a network, a method, comprising: receiving data transmitted via the network (e.g., 410, Fig. 4; page 14, lines 7-17); identifying first data that may contain malicious content (e.g., 420, 440, Fig. 4; page 14, line 18 – page 16, line 2); generating report information based on the first data (e.g., 440, Fig. 4; page 15, line 18 – page 16, line 2); forwarding the report information to an external device when the report information indicates that the first data potentially contains malicious content, the report information allowing the external device to make a forwarding decision on behalf of the network device (e.g., 510, 520, Fig. 5; page 16, line 20 – page 17, line 11); and forwarding the first data to the user

device when it is determined that the first data does not contain malicious content (e.g., 470, Fig. 4; page 16, lines 3-9).

Claim 13 recites: The method of claim 10, further comprising: receiving, from the external device, information indicating whether the first data is to be forwarded to the user device (e.g., 520, Fig. 5; page 17, lines 7-11); and dropping the first data when the information indicates that the first data is not to be forwarded (e.g., 530, Fig. 5; page 17, lines 12-18).

Claim 15 recites: The method of claim 10, wherein the identifying comprises: identifying spam (e.g., page 7, line 17 – page 8, line 7).

Claim 16 recites: A computer-readable medium having stored thereon a plurality of sequences of instructions, said sequences of instructions including instructions which, when executed by a processor, cause the processor to: receive data transmitted via a network (e.g., 410, Fig. 4; page 14, line 7-17); receive at least one set of rules from an external device, the at least one set of rules being associated with processing the received data (e.g., 420, Fig. 4; page 14, line 18 – page 15, line 4); determine whether the data may contain malicious content using a first set of rules (e.g., 420, Fig. 4; page 14, line 18 – page 15, line 4); identify first data that may contain malicious content based on the determining (e.g., 420, Fig. 4; page 14, line 18 – page 15, line 4); generate report information based on the first data (e.g., 440, Fig. 4; page 15, line 18 – page 16, line 9); forward the first data for processing by a user application when the report information indicates that the first data does not contain malicious content (e.g., 470, Fig. 4; page 16, lines 3-9); and forward the report information to an external device when the report information indicates that the first data potentially contains malicious content, the report

information allowing the external device to make a forwarding decision on behalf of the processor (e.g., 510, 520; Fig. 5; page 16, line 20 – page 17, line 11).

Claim 21 recites: The computer-readable medium of claim 20, wherein when identifying first data that may contain malicious content, the instructions cause the processor to identify spam (e.g., page 7, line 17 – page 8, line 7).

Claim 22 recites: The computer-readable medium of claim 16, wherein the instructions further cause the processor to execute the received data, the data being associated with at least one of video-on-demand, video-based training, on-line gaming, on-line shopping, downloading music files or downloading games (e.g., page 13, lines 15-19).

VI.   GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

A.   Claims 1, 4, 5, 8-10, 12-14, 16, 19, and 20 stand rejected under 35 U.S.C.

§ 103(a) as being unpatentable over SCHNEIER et al. (U.S. Patent Application

Publication No. 2002/0087882) in view of JOYCE (U.S. Patent No. 6,519,703).

B.   Claims 6, 15, and 21 stand rejected under 35 U.S.C. § 103(a) as being

unpatentable over SCHNEIER et al. in view of JOYCE and further in view of JUDGE

(U.S. Patent No. 6,941,467).

C.   Claims 7 and 22 stand rejected under 35 U.S.C. § 103(a) as being

unpatentable over SCHNEIER et al. in view of JOYCE and further in view of BATES et

al. (U.S. Patent No. 6,785,732).

VII.   ARGUMENT

A.   The rejection of claims 1, 4, 5, 8-10, 12-14, 16, 19, and 20 under 35
U.S.C. § 103 based on SCHNEIER et al. and JOYCE should be reversed.

The initial burden of establishing a *prima facie* basis to deny patentability to a

claimed invention always rests upon the Examiner. In re Oetiker, 977 F.2d 1443, 24

U.S.P.Q.2d 1443 (Fed. Cir. 1992). In rejecting a claim under 35 U.S.C. § 103, the

Examiner must provide a factual basis to support the conclusion of obviousness. In re

Warner, 379 F.2d 1011, 154 U.S.P.Q. 173 (C.C.P.A. 1967). Based upon the objective

evidence of record, the Examiner is required to make the factual inquiries mandated by

Graham v. John Deere Co., 86 S. Ct. 684, 383 U.S. 1, 148 U.S.P.Q. 459 (1966). KSR

International Co. v. Teleflex Inc., 550 U.S. 398, 127 S. Ct. 1727 (2007). The Examiner is

also required to explain how and why one having ordinary skill in the art would have

been realistically motivated to modify an applied reference and/or combine applied

references to arrive at the claimed invention. Uniroyal, Inc. v. Rudkin-Wiley Corp., 837

F.2d 1044, 5 U.S.P.Q.2d 1434 (Fed. Cir. 1988).

1.   Claims 1, 4, 5, 8, and 9

Independent claim 1 recites a device that includes at least one interface configured

to receive data transmitted via a network; a firewall configured to: receive data from the

at least one interface, determine whether the data potentially contains malicious content,

and identify first data in the received data that potentially contains malicious content;

intrusion detection logic configured to: receive the first data, and generate report

information based on the first data; and forwarding logic configured to: receive the report

information, forward the first data for processing by a user application when the report

information indicates that the first data does not contain malicious content; and forward

the report information to a remote central management system when the report

information indicates that the first data potentially contains malicious content, the report

information allowing the remote central management system to make a forwarding

decision on behalf of the device. SCHNEIER et al. and JOYCE, whether taken alone or

in any reasonable combination, do not disclose or suggest this combination of features.

For example, SCHNEIER et al. and JOYCE do not disclose or suggest forwarding

logic configured to forward report information to a remote central management system

when the report information indicates that first data potentially contains malicious

content, the report information allowing the remote central management system to make

a forwarding decision on behalf of the device. The Examiner relies on paragraphs 0064

and 0068 of SCHNEIER et al. as allegedly disclosing this feature (Office Action, pp. 4

and 5). Appellants respectfully disagree with the Examiner's interpretation of

SCHNEIER et al.

At paragraph 0064, SCHNEIER et al. discloses:

FIG. 2 is a system overview of an exemplary embodiment of a probe/sentry
system. One or more such systems can be installed at each customer site to
monitor the customer's network and network components. (A database of all
network components monitored by such probe/sentry systems may be stored by
SOCRATES 6000 in a database similar to that suggested in TABLE 7 of
Appendix C.) Data collected by sensors 1010, 1020, 1030 and 1040 (note that
four sensors are shown solely by way of example and are not meant to limit the
scope of the invention) are collated by sensor data collator 2010. Once collated,
the data is first filtered by negative filtering subsystem 2020, which discards
uninteresting information, and then by positive filtering subsystem 2030, which
selects possibly interesting information and forwards it to communications and
resource coordinator 2060. Data neither discarded by negative filtering
subsystem 2020 nor selected out as interesting by positive filtering subsystem
2030 form the "residue," which is sent to anomaly engine 2050 for further
analysis. Anomaly engine 2050 determines what residue information may be
worthy of additional analysis and sends such information to communications and
resource coordinator 2060 for forwarding to the SOC. Negative filtering, positive
filtering, and residue analysis are examples of data discrimination analyses, other
types of which are well-known to those skilled in the art.

This section of SCHNEIER et al. discloses a probe/sentry system that analyzes and acts on interesting data or anomalies by filtering data using a negative filtering subsystem to discard uninteresting information and then filtering the data by a positing filtering subsystem, which selects possibly interesting information and forwards it to a communications and resource coordinator for forwarding to a security operations center (SOC). The communications and resource coordination then creates sentry messages out of the interesting status data and forwards those messages on to a gateway system within the SOC (paragraph 0065). Gateway messages arrive at SOCRATES, within the SOC, from the gateway system, where event records are stored and linked with other even records to form "problem tickets," which are then opened and displayed on security analyst consoles for handling by security analysts (paragraph 0085).

Therefore, SCHNEIER et al. discloses that, when possibly interesting information is selected, the information is matched with other information and displayed on security analyst consoles. Assuming, for the sake of argument, that the interesting information of SCHNEIER et al. can reasonably be construed as the first data of claim 1 and that the SOC can reasonably be construed as the remote central management system of claim 1 (points that Appellants do not concede), SCHNEIER et al. does not disclose forwarding logic configured to forward report information to the SOC when the report information indicates that the interesting information potentially contains malicious content, the report information allowing the SOC to make a forwarding decision on behalf of the device, as would be required by SCHNEIER et al. based on the Examiner's interpretation of claim 1. Instead, as noted above, at the SOC, problem tickets are formed for handling by security analysts. Because SCHNEIER et al. discloses a probe/sentry system that

<u>monitors and collects information</u> concerning the status of a network and its components

(paragraph 0035), there would be no reason for the <u>sentry system</u> of SCHNEIER et al. to

make <u>forwarding decisions</u>. Therefore, this section of SCHNEIER et al. does not

disclose or suggest forwarding logic configured to forward report information to a remote

central management system when the report information indicates that first data

potentially contains malicious content, the report information allowing the remote central

management system to make a forwarding decision on behalf of the device, as recited in

claim 1.

> At paragraph 0068, SCHNEIER et al. discloses:

>> Network response subsystem 2070 can, among other things, process and execute
>> requests originating from the SOC designed to mitigate or terminate various
>> attacks. For example, network response subsystem 2070 might be requested by
>> the SOC via Pipes 3000 to not allow a certain IP address to access the customer's
>> network for the next 10 minutes. Such a "fix" might be sufficient to stop a
>> transient attack, such as someone repeatedly trying to log in to the customer's
>> network.

This section of SCHNEIER et al. discloses <u>blocking a certain IP address</u> from accessing a

customer's network. This section of SCHNEIER et al. has nothing to do with a remote

central management system that makes a forwarding decision on behalf of a device. In

fact, this section of SCHNEIER et al. has nothing to do with making a forwarding

decision at all. Therefore, this section of SCHNEIER et al. does not disclose or suggest

forwarding logic configured to forward report information to a remote central

management system when the report information indicates that first data potentially

contains malicious content, the report information allowing the remote central

management system to make a forwarding decision on behalf of the device, as recited in

claim 1.

Appellants submit that the disclosure of JOYCE does not remedy the deficiencies in the disclosure of SCHNEIER et al. set forth above with respect to claim 1.

For at least the foregoing reasons, Appellants submit that the rejection of claim 1 under 35 U.S.C. § 103(a) based on SCHNEIER et al. and JOYCE is improper. Accordingly, Appellants request that the rejection be reversed.

Claims 4, 5, 8, and 9 depend from claim 1. Therefore, Appellants request that the rejection of these claims be reversed for at least the reasons given above with respect to claim 1.

> 2. <u>Claims 10 and 12-14</u>

Independent claim 10 recites a method in a network device configured to receive data transmitted over a network. The method includes receiving data transmitted via the network; identifying first data that may contain malicious content; generating report information based on the first data; forwarding the report information to an external device when the report information indicates that the first data potentially contains malicious content, the report information allowing the external device to make a forwarding decision on behalf of the network device; and forwarding the first data to the user device when it is determined that the first data does not contain malicious content. SCHNEIER et al. and JOYCE, whether taken alone or in any reasonable combination, do not disclose or suggest this combination of features.

For example, SCHNEIER et al. and JOYCE do not disclose or suggest forwarding report information to an external device when the report information indicates that first data potentially contains malicious content, the report information allowing the external device to make a forwarding decision on behalf of the network device. The Examiner

relies on paragraphs 0064 and 0068 of SCHNEIER et al. as allegedly disclosing this feature (Office Action, pp. 7 and 8). Appellants respectfully disagree with the Examiner's interpretation of SCHNEIER et al.

As noted above, at paragraph 0064, SCHNEIER et al. discloses a probe/sentry system that analyzes and acts on interesting data or anomalies by filtering data using a negative filtering subsystem to discard uninteresting information and then filtering the data by a positing filtering subsystem, which selects possibly interesting information and forwards it to a communications and resource coordinator for forwarding to the SOC. The communications and resource coordination then creates sentry messages out of the interesting status data and forwards those messages on to a gateway system within the SOC (paragraph 0065). Gateway messages arrive at SOCRATES, within the SOC, from the gateway system, where event records are stored and linked with other even records to form "problem tickets," which are then opened and displayed on security analyst consoles for handling by security analysts (paragraph 0085).

Therefore, SCHNEIER et al. discloses that, when possibly interesting information is selected, the information is matched with other information and displayed on security analyst consoles. Assuming, for the sake of argument, that the interesting information of SCHNEIER et al. can reasonably be construed as the first data of claim 10 and that the SOC can reasonably be construed as the external device of claim 10 (points that Appellants do not concede), SCHNEIER et al. does not disclose forwarding report information to the SOC when the report information indicates that the interesting information potentially contains malicious content, the report information allowing the SOC to make a forwarding decision on behalf of the network device, as would be

required by SCHNEIER et al. based on the Examiner's interpretation of claim 10. Instead, as noted above, at the SOC, problem tickets are formed for handling by security analysts. Because SCHNEIER et al. discloses a probe/sentry system that <u>monitors and collects information</u> concerning the status of a network and its components (paragraph 0035), there would be no reason for the <u>sentry system</u> of SCHNEIER et al. to make <u>forwarding decisions</u>. Therefore, this section of SCHNEIER et al. does not disclose or suggest forwarding report information to an external device when the report information indicates that first data potentially contains malicious content, the report information allowing the external device to make a forwarding decision on behalf of the network device, as recited in claim 10.

As noted above, at paragraph 0068, SCHNEIER et al. discloses <u>blocking a certain IP address</u> from accessing a customer's network. This section of SCHNEIER et al. has nothing to do with an external device that makes a forwarding decision on behalf of a network device. In fact, this section of SCHNEIER et al. has nothing to do with making a forwarding decision at all. Therefore, this section of SCHNEIER et al. does not disclose or suggest forwarding report information to an external device when the report information indicates that first data potentially contains malicious content, the report information allowing the external device to make a forwarding decision on behalf of the network device, as recited in claim 10.

Appellants submit that the disclosure of JOYCE does not remedy the deficiencies in the disclosure of SCHNEIER et al. set forth above with respect to claim 10.

For at least the foregoing reasons, Appellants submit that the rejection of claim 10 under 35 U.S.C. § 103(a) based on SCHNEIER et al. and JOYCE is improper.

Accordingly, Appellants request that the rejection be reversed.

Claims 12-14 depend from claim 10. Therefore, Appellants request that the rejection of these claims be reversed for at least the reasons given above with respect to claim 10.

3. Claims 16, 19, and 20

Independent claim 16 recites a computer-readable medium having stored thereon a plurality of sequences of instructions. The sequences of instructions include instructions which, when executed by a processor, cause the processor to: receive data transmitted via a network; receive at least one set of rules from an external device, the at least one set of rules being associated with processing the received data; determine whether the data may contain malicious content using a first set of rules; identify first data that may contain malicious content based on the determining; generate report information based on the first data; forward the first data for processing by a user application when the report information indicates that the first data does not contain malicious content; and forward the report information to an external device when the report information indicates that the first data potentially contains malicious content, the report information allowing the external device to make a forwarding decision on behalf of the processor. SCHNEIER et al. and JOYCE, whether taken alone or in any reasonable combination, do not disclose or suggest this combination of features.

For example, SCHNEIER et al. and JOYCE do not disclose or suggest a processor to forward the report information to an external device when the report information indicates that the first data potentially contains malicious content, the report information allowing the external device to make a forwarding decision on behalf of the

processor. The Examiner relies on paragraphs 0064 and 0068 of SCHNEIER et al. as

allegedly disclosing this feature (Office Action, pp. 11 and 12). Appellants respectfully

disagree with the Examiner's interpretation of SCHNEIER et al.

As noted above, at paragraph 0064, SCHNEIER et al. discloses a probe/sentry

system that analyzes and acts on interesting data or anomalies by filtering data using a

negative filtering subsystem to discard uninteresting information and then filtering the

data by a positing filtering subsystem, which selects possibly interesting information and

forwards it to a communications and resource coordinator for forwarding to the SOC.

The communications and resource coordination then creates sentry messages out of the

interesting status data and forwards those messages on to a gateway system within the

SOC (paragraph 0065). Gateway messages arrive at SOCRATES, within the SOC, from

the gateway system, where event records are stored and linked with other even records to

form "problem tickets," which are then opened and displayed on security analyst

consoles for handling by security analysts (paragraph 0085).

Therefore, SCHNEIER et al. discloses that, when possibly interesting information

is selected, the information is matched with other information and displayed on security

analyst consoles. Assuming, for the sake of argument, that the interesting information of

SCHNEIER et al. can reasonably be construed as the first data of claim 16 and that the

SOC can reasonably be construed as the external device of claim 16 (points that

Appellants do not concede), SCHNEIER et al. does not disclose a processor to forward

report information to the SOC when the report information indicates that the interesting

information potentially contains malicious content, the report information allowing the

SOC to make a forwarding decision on behalf of the processor, as would be required by

SCHNEIER et al. based on the Examiner's interpretation of claim 16. Instead, as noted above, at the SOC, problem tickets are formed for handling by security analysts. Because SCHNEIER et al. discloses a probe/sentry system that <u>monitors and collects information</u> concerning the status of a network and its components (paragraph 0035), there would be no reason for the <u>sentry system</u> of SCHNEIER et al. to make <u>forwarding decisions</u>. Therefore, this section of SCHNEIER et al. does not disclose or suggest a processor to forward the report information to an external device when the report information indicates that the first data potentially contains malicious content, the report information allowing the external device to make a forwarding decision on behalf of the processor, as recited in claim 16.

As noted above, at paragraph 0068, SCHNEIER et al. discloses <u>blocking a certain IP address</u> from accessing a customer's network. This section of SCHNEIER et al. has nothing to do with an external device that makes a forwarding decision on behalf of a network device. In fact, this section of SCHNEIER et al. has nothing to do with making a forwarding decision at all. Therefore, this section of SCHNEIER et al. does not disclose or suggest a processor to forward the report information to an external device when the report information indicates that the first data potentially contains malicious content, the report information allowing the external device to make a forwarding decision on behalf of the processor, as recited in claim 16.

Appellants submit that the disclosure of JOYCE does not remedy the deficiencies in the disclosure of SCHNEIER et al. set forth above with respect to claim 16.

For at least the foregoing reasons, Appellants submit that the rejection of claim 16 under 35 U.S.C. § 103(a) based on SCHNEIER et al. and JOYCE is improper.

Accordingly, Appellants request that the rejection be reversed.

Claims 19 and 20 depend from claim 16. Therefore, Appellants request that the rejection of these claims be reversed for at least the reasons given above with respect to claim 16.

     B.   The rejection of claims 6, 15, and 21 under 35 U.S.C. § 103 based on SCHNEIER et al., JOYCE, and JUDGE should be reversed.

     1.   Claim 6

Claim 6 depends from claim 5. Without acquiescing in the Examiner's rejection of claim 6, Appellants submit that the disclosure of JUDGE does not remedy the deficiencies in the disclosures of SCHNEIER et al. and JOYCE set forth above with respect to claim 5. Therefore, Appellants request that the rejection of claim 6 be reversed for at least the reasons given above with respect to claim 5.

     2.   Claim 15

Claim 15 depends from claim 10. Without acquiescing in the Examiner's rejection of claim 15, Appellants submit that the disclosure of JUDGE does not remedy the deficiencies in the disclosures of SCHNEIER et al. and JOYCE set forth above with respect to claim 10. Therefore, Appellants request that the rejection of claim 15 be reversed for at least the reasons given above with respect to claim 10.

     3.   Claim 21

Claim 21 depends from claim 16. Without acquiescing in the Examiner's rejection of claim 21, Appellants submit that the disclosure of JUDGE does not remedy the deficiencies in the disclosure of SCHNEIER et al. and JOYCE set forth above with respect to claim 16. Therefore, Appellants request that the rejection of claim 21 be reversed for at least the reasons given above with respect to claim 16.

C.   The rejection of claims 7 and 22 under 35 U.S.C. § 103 based on
        SCHNEIER et al., JOYCE, and BATES et al. should be reversed.

        1.   Claim 7

Claim 7 depends from claim 1. Without acquiescing in the Examiner's rejection

of claim 7, Appellants submit that the disclosure of BATES et al. does not remedy the

deficiencies in the disclosures of SCHNEIER et al. and JOYCE set forth above with

respect to claim 1. Therefore, Appellants request that the rejection of claim 7 be reversed

for at least the reasons given above with respect to claim 1.

        2.   Claim 22

Claim 22 depends from claim 16. Without acquiescing in the Examiner's

rejection of claim 22, Appellants submit that the disclosure of BATES et al. does not

remedy the deficiencies in the disclosures of SCHNEIER et al. and JOYCE set forth

above with respect to claim 16. Therefore, Appellants request that the rejection of claim

22 be reversed for at least the reasons given above with respect to claim 16.

VIII.   CONCLUSION

In view of the foregoing arguments, Appellants respectfully solicit the Honorable Board to reverse the Examiner's rejections of claims 1, 4-10, 12-16, and 19-22.

To the extent necessary, a petition for an extension of time under 37 C.F.R. § 1.136 is hereby made. Please charge any shortage in fees due in connection with the filing of this paper, including extension of time fees, to Deposit Account 50-1070 and please credit any excess fees to such deposit account.

Respectfully submitted,

HARRITY & HARRITY, LLP

By: /Meagan S. Walling, Reg. No. 60,112/
    Meagan S. Walling
    Reg. No. 60,112

Date: January 26, 2009

11350 Random Hills Road
Suite 600
Fairfax, VA 22030
Telephone: (571) 432-0800
Facsimile: (571) 432-0808

CUSTOMER NUMBER: 25537

IX.   CLAIM APPENDIX

1. A device, comprising:

at least one interface configured to receive data transmitted via a network;

a firewall configured to:

    receive data from the at least one interface,

    determine whether the data potentially contains malicious content, and

    identify first data in the received data that potentially contains malicious content;

intrusion detection logic configured to:

    receive the first data, and

    generate report information based on the first data; and

forwarding logic configured to:

    receive the report information,

    forward the first data for processing by a user application when the report information indicates that the first data does not contain malicious content; and

    forward the report information to a remote central management system when the report information indicates that the first data potentially contains malicious content, the report information allowing the remote central management system to make a forwarding decision on behalf of the device.

4. The device of claim 1, further comprising:

a virtual private network gateway configured to establish a secure connection with the remote central management system.

5. The device of claim 1, wherein the firewall comprises anti-virus logic configured to examine a data stream for viral signatures using at least one of a signature-based technique, a heuristic technique or a rough set logic technique.

6. The device of claim 5, wherein the anti-virus logic is further configured to identify unsolicited messages.

7. The device of claim 1, further comprising:

a processing device executing the user application, the user application being associated with at least one of video-on-demand, video-based training, on-line gaming, on-line shopping, downloading music files or downloading games.

8. The device of claim 1, wherein at least one of the firewall, the intrusion detection logic or the forwarding logic is configured to receive rule-based processing information from an external device via the network.

9. The device of claim 8, wherein at least one of the firewall, intrusion detection logic or forward logic is further configured to receive updated rule-based processing information from the external device.

10. In a network device configured to receive data transmitted over a network, a method, comprising:

receiving data transmitted via the network;

identifying first data that may contain malicious content;

generating report information based on the first data;

forwarding the report information to an external device when the report information indicates that the first data potentially contains malicious content, the report information allowing the external device to make a forwarding decision on behalf of the network device; and

forwarding the first data to the user device when it is determined that the first data does not contain malicious content.

12. The method of claim 10, further comprising:

establishing a virtual private network connection to the external device, and wherein the forwarding the report information includes:

forwarding the report information over the virtual private network connection.

13. The method of claim 10, further comprising:

receiving, from the external device, information indicating whether the first data is to be forwarded to the user device; and

dropping the first data when the information indicates that the first data is not to be forwarded.

14. The method of claim 10, wherein the identifying comprises:

examining the received data for viruses using at least one of a signature-based technique, a heuristic technique or a rough set logic-based technique.

15. The method of claim 10, wherein the identifying comprises:

identifying spam.

16. A computer-readable medium having stored thereon a plurality of sequences of instructions, said sequences of instructions including instructions which, when executed by a processor, cause the processor to:

receive data transmitted via a network;

receive at least one set of rules from an external device, the at least one set of rules being associated with processing the received data;

determine whether the data may contain malicious content using a first set of rules;

identify first data that may contain malicious content based on the determining;

generate report information based on the first data;

forward the first data for processing by a user application when the report information indicates that the first data does not contain malicious content; and

forward the report information to an external device when the report information indicates that the first data potentially contains malicious content, the report information allowing the external device to make a forwarding decision on behalf of the processor.

19. The computer-readable medium of claim 16, wherein the instructions further cause the processor to:

establish a virtual private network tunnel with the external device and send the report information over the virtual private network tunnel.

20. The computer-readable medium of claim 16, wherein when identifying first data that may contain malicious content, the instructions cause the processor to identify a virus using at least one of a signature-based technique, a heuristic technique or a rough set logic-based technique.

21. The computer-readable medium of claim 20, wherein when identifying first data that may contain malicious content, the instructions cause the processor to identify spam.

22. The computer-readable medium of claim 16, wherein the instructions further cause the processor to execute the received data, the data being associated with at least one of video-on-demand, video-based training, on-line gaming, on-line shopping, downloading music files or downloading games.

X.   EVIDENCE APPENDIX

None

XI.   RELATED PROCEEDINGS APPENDIX

None